Symantec(TM) Encryption Management Server Version 3.3 Release Notes

Thank you for using this Symantec Corporation product. These Release Notes contain important information regarding this release of Symantec Encryption Management Server. Symantec Corporation strongly recommends you read this entire document.

Symantec Corporation welcomes your comments and suggestions. You can use the information in Getting Assistance to contact us.

Product: Symantec Encryption Management Server

Version: 3.3.1

Warning: Export of this software may be restricted by the U.S. government.

Note: To view the most recent version of this document, go to the Products section on the Symantec Corporation Support website.

About Symantec Encryption Management Server

Symantec Encryption Management Server provides your enterprise with secure messaging by transparently protecting your messages without user interaction. It automatically creates and maintains a Self-Managing Security Architecture (SMSA) by monitoring authenticated users and their email traffic. You can also send protected messages to addresses that are not part of the SMSA.

The Symantec Encryption Management Server encrypts, decrypts, signs, verifies messages, and provides strong security through policies you control. Symantec Encryption Satellite provides security for email messages up to the email user's computer, allows external users to become part of the SMSA, and provides end users the option to create and manage their keys on their computers.

Symantec Encryption Management Server Technology Partner Edition

Many of the features described in the documentation are not available in the Symantec Encryption Management Server Technology Partner Edition. To upgrade to the full version of Symantec Encryption Management Server, go to the Symantec Home Page.

You can determine whether you have this version by looking in the **Server Information** panel of the **General Settings** page.

Common Criteria Environments

To be Common Criteria compliant, review the best practices in *PGP Universal Server 2.9 Common Criteria Supplemental*. These best practices supersede recommendations made elsewhere in this and other documentation.

What's Included in This File

- About Symantec Encryption Management Server
- Changes in This Release
- System Requirements
- Upgrade/Migration Requirements
- Additional Information
- Getting Assistance
- Copyright and Trademarks

Changes in This Release

This section lists the changes in this release of Symantec Encryption Management Server.

Upgrade/Migration Issues

Warning: Before you migrate to version 3.3.1, to avoid issues after the migration, the following circumstances may require actions on your system:
-If you are using a hardware token ignition key or a Hardware Security Module (HSM) with a software version before 3.3, including a migration (backup/upgrade/restore) from 3.0.0.
-If you are migrating a 2.x cluster to version 3.3.1.
See the warnings in the following section "Upgrade/Migration Requirements" or read *Symantec Encryption Management Server Upgrade Guide* before you upgrade or migrate. Contact Technical Support if you have questions.

What's New in Symantec Encryption Management Server 3.3

Symantec Encryption Management Server 3.3.1 introduces the following new and improved features:

- **Compatibility with VMware ESXi 5.1**

  This release provides installation of Symantec Encryption Management Server on VMware ESX virtual machines running ESXi 5.1.

- **Compatibility with New Linux Packages**

  This release supports the installation of Symantec Drive Encryption for Linux on Ubuntu 12.04 LTS (32-bit and 64-bit versions) and Red Hat Enterprise Linux/CentOS 5.9, 6.3, and 6.4 (32-bit and 64-bit versions).

- **Compatibility with Apple Mac OS X 10.8.2, 10.8.3, and 10.8.4**

  This release supports installation of Symantec Encryption Desktop on systems running Mac OS X 10.8.2, 10.8.3, and 10.8.4 (Mountain Lion).

- **Compatibility with Microsoft Windows 8**

  This release supports the installation of Symantec Encryption Desktop on systems running Microsoft Windows 8 Pro and Microsoft Windows 8 Enterprise, both 32- and 64-bit versions.

- **Compatibility with Microsoft Outlook 2013**

  Symantec Encryption Desktop is now compatible with Microsoft Office 2013, both 32- and 64-bit versions.

- **Compatibility with Microsoft Office 365 Cloud Server**

  Symantec Encryption Desktop is now compatible with Microsoft Office 365 Server when you are using a supported email client. Note that encrypted email is not supported if you are using a web-based email client with Office 365 Cloud Server.

Symantec Encryption Management Server 3.3.0 introduces the following new and improved features:

- **Symantec identity branding**

  The PGP product line has been renamed. For a detailed map of old product names to new ones, refer to the Symantec Knowledgebase article TECH197084.

- **Integration with Symantec File Share Encryption and Dropbox on Apple iOS devices**

  The integration of Symantec File Share Encryption, formerly known as PGP NetShare, with Dropbox brings protection to files copied from a Dropbox Windows client to cloud-based storage. You can then view these encrypted Dropbox files on your iOS device. This integration allows protected files to move among Dropbox locations, to be read, edited, and saved by you or a collaborative group. Files and folders are encrypted or decrypted transparently, as needed.

- **Gateway Email Integration with Symantec Data Loss Prevention**

  Symantec Gateway Email, previously known as PGP Universal Gateway Email, has deepened its integration with Symantec Data Loss Prevention and Symantec Messaging Gateway powered by Brightmail. Symantec Messaging Gateway sends outbound email to Data Loss Prevention, which scans the email, flags the message for security violations or sensitivity. The flagged email gets routed to GWE to process corresponding security remediation through mail policy. Symantec Gateway Email then sends encryption remediation status confirmation back to Data Loss Prevention. Audit information is centrally located in Data Loss Prevention Enforce. This status synchronization leverages Data Loss Prevention's new Incident Remediation API (IRA). This new feature is called Email Encryption Connect in DLP Enforce.

- **Next generation of mobile email management**

  PGP Viewer, which has been renamed to Symantec Mobile Encryption for iOS, now expands the ability beyond viewing to securely reply to encrypted messages or initiate new secure messages, with or without attachments. Mobile Encryption for iOS integrates with Microsoft Exchange Mobile Address List for access to your email contacts. PGP Viewer 1.0 users can automatically update to Mobile Encryption for iOS version 2.0. This product requires the mobile management policy provided in Symantec Encryption Management Server 3.3.

- **Expanded Platform Compatibility for Symantec Web Email Protection**

  Email sent using the Symantec Web Email Protection feature, formerly known as PGP Web Messenger, can now be viewed using a browser on most iOS and Android mobile devices

- **Expanded Platform Compatibility for Symantec PDF Email Protection**

  Email sent using the Symantec PDF Email Protection feature, formerly PGP PDF Messenger, can now be viewed using a browser on most iOS and Android mobile devices.

- **Compatibility with VMware ESXi 5**

  This release provides installation of Symantec Encryption Management Server, formerly known as PGP Universal Server, on VMware ESX virtual machines running ESXi 5.

- **Compatibility with New Linux Packages**

  This release supports installation of Symantec Drive Encryption for Linux, formerly known as PGP Whole Disk Encryption for Linux, on Red Hat Enterprise Linux/CentOS 6.1 and 6.2 (32-bit and 64-bit versions).

- **Compatibility with Apple Mac OS X 10.8**

  This release supports installation of Symantec Desktop Encryption, formerly known as PGP Desktop, on systems running Mac OS X 10.8 (Mountain Lion).

- **Win PE 64-bit Support**

  Symantec Drive Encryption, formerly known as PGP Whole Disk Encryption, now provides WinPE recovery for both 32-bit and 64-bit Windows 7 environments.

- **Removal of the PGP Remote Disable and Destroy Feature**

  Symantec Corporation has discontinued the PGP Remote Disable and Destroy (RDD) feature, including its policy management and reporting functionalities. However, the feature is retained for customers who have an existing subscription entitlement until their current subscription period expires. For information on how to disable PGP RDD, go to the Symantec Knowledgebase and search for article ID HOWTO79556, "HOW TO: Remove PGP Remote Disable and Destroy (PGP RDD)".

Resolved Issues

For a list of issues that have been resolved in this release, please go to the Symantec Knowledgebase and search for TECH164863, "Symantec Encryption Management Server Resolved Issues."

System Requirements

Symantec Encryption Management Server is a customized Linux OS installation and cannot be installed on a Windows server. Every Symantec Encryption Management Server requires a dedicated system that meets the system requirements listed below. The installation process deletes all data on the system and reconfigures it as a Symantec Encryption Management Server.

Symantec Encryption Management Server Certified Hardware List - Valid September 17, 2013 through September 17, 2014

You must obtain the latest version of this list for hardware purchasing decisions after September 17, 2014.

The following systems are certified as the hardware for Symantec Encryption Management Server:

- **Dell PowerEdge R320** - Intel XEON E5-2430 @ 2.2 GHz - 12 GB RAM
  Two 500 GB 7200 RPM SATA - PERC H310 Internal HD controller
  Broadcom BCM5720 network controller
  Small/medium environment production unit
- **Dell PowerEdge R720** - Two Intel XEON E5-2640 @ 2.5 GHz – 16 GB RAM
  Two 300 GB 10K RPM SAS - PERC H310 RAID
  Broadcom BCM5720 network controller
  Medium/large environment production unit, cluster member
- **IBM BladeCenter HS22** - Two Intel XEON E5607 @ 2.4 GHz - 16 GB RAM
  Two 300 GB 10K 6 Gbps SAS - ServeRAID MR10ie RAID
  Intel 10-Gigabit 82599EB chipset network controller
  Medium/large environment production unit, cluster member
- **IBM System x3250 M4** - Intel XEON E3-1230 @ 3.3 GHz - 16 GB RAM
  Two 300 GB 10K 6Gbps SAS 2.5" - ServeRAID H1110 RAID
  Broadcom NetXtreme i Quad Port GbE with BCM5709 chipset network controller
  Medium/large environment production unit, cluster member
- **IBM System x3650 M4** - Two Intel XEON E5-2630 @ 2.3 GHz - 16 GB RAM
  Four 300 GB SAS 10K RPM - IBM ServeRAID-M5110e RAID
  Intel I350 network controller
  Medium/large environment production unit, cluster member
- **HP Proliant DL120 G7** - Intel XEON E3-1230 @ 3.2 GHz - 16 GB RAM
  Two 250 GB 7200 RPM SATA - Smart Array B110i RAID
  Intel 82574L network controller
  Small/medium environment production unit
- **HP Proliant DL385 G7**- Two AMD Opteron 6234 @ 2.4 GHz - 16 GB RAM
  Two 300 GB 15K RPM SAS - HP Smart Array P410i RAID
  Broadcom BCM5709 network controller
  Medium/large environment production unit, cluster member
- **VMWare vSphere 5.1** - Supported platform, non-hardware.
  Sufficient processing power equivalent to a 3 GHz Intel Xeon must be dedicated to the Symantec Encryption Management Server virtual machine.

VMware Tools must be installed and configured in the Symantec Encryption Management Server operating system.
Disk space requirements:

- Small/medium environment - 50 GB minimum allocated to the VMware instance; 4 GB RAM dedicated to the VMware instance.
- Medium/large environment - 100 GB minimum allocated to the VMware instance; 8 GB RAM dedicated to the VMware instance.

- **VMWare vSphere Hypervisor (ESXi) 5.1 with VMotion Support** - Supported platform, non-hardware
  - VMware HA Configuration: Host Monitoring - Enabled; VM Monitoring - Disabled; Application Monitoring - Disabled
  - VMware DRS Configuration: Migration Automation Level - Fully automated; Power Management Automation Level - Off; Migration Threshold - Apply all recommendations.

Although a broad array of other hardware may work well with Symantec Encryption Management Server, Symantec Encryption Management Server has been tested with, and is compatible with, the systems in this list.

Note: Symantec Encryption Management Server supports additional memory beyond the minimum requirement but not exceeding 16 gigabytes.

To qualify as Symantec Encryption Management Server Certified Hardware, the server must be one of the versions listed and all components must be configured as specified. For Support purposes, if you change the sizes of hard disks in the same type of drive (for example, 36 GB SCSI to 73 GB SCSI), increasing memory configurations and processor speeds in the same type and family qualifies as the same system.

Supported Client and Symantec Encryption Management Server Version Combinations

Symantec Corporation supports backward compatibility for clients only. Symantec Encryption Management Server 3.3.1 supports managing policy of these versions and subsequent maintenance releases for each of the following:

PGP Desktop

- 10.0.0
- 10.0.1
- 10.0.2
- 10.1.0
- 10.2.0
- 10.2.1

Symantec Encryption Desktop

- 10.3.0
- 10.3.1

Note: Limited backward compatibility support means that legacy features, such as enrollment, policy download, logging and reporting are supported, but legacy clients cannot access the latest client features in Consumer Policy.

We recommend that you upgrade your Symantec Encryption Management Server and your clients, so that they are eventually on the same release. For the most current information on which client versions are supported, see the Knowledge Base.

Mailserver Requirements

Symantec Encryption Management Server supports the following mailservers:

- Microsoft Exchange 2010 SP1
- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2003 SP2
- Lotus Domino Server 8.5.2
- Lotus Domino Server 8.5.3

Mailservers *not* on this list may not be fully compatible or supported.

Microsoft Exchange Server 5.5 is not a supported mailserver and has known incompatibilities, such as with LDAP Directory Synchronization.

Symantec Encryption Management Server Administrative Interface Web Browser Requirements

The Symantec Encryption Management Server administrative interface has been fully tested with the following Web browsers:

Windows	■ Internet Explorer 7 and greater On Microsoft Windows Server 2012 systems, the **Allow META REFRESH** option is disabled by default. This option must be enabled for the web interface to work correctly with Internet Explorer 10. If you are using Internet Explorer on Windows Server 2012, from **Tools > Internet Options**, select the **Security** tab and click **Custom level**. Enable **Miscellaneous > Allow META REFRESH**. ■ Firefox 12 and greater
Mac OS X	■ Safari 5.1 and greater ■ Firefox 16 and greater

Although the administrative interface works with other Web browsers, we recommend these browsers for maximum compatibility.

Symantec Encryption Web Email Protection Web Browser Requirements

Windows	Internet Explorer 7 and greater Firefox 12 and greater
Mac OS X	Safari 5.1 and greater Firefox 16 and greater

Supported Mobile Platforms for Symantec Encryption Web Email Protection and Symantec Encryption PDF Email Protection

Symantec Encryption Web Email Protection and Symantec Encryption PDF Email Protection support the following platforms for Smartphones and Tablets:

Feature	Operating System	Device	Web Browser
Symantec Encryption Web Email Protection/Symantec Encryption PDF Email Protection for smartphones	Android 2.3.6	Samsung Galaxy S II	Default Android 2 Browser
	iOS 5.0.1	iPhone 4S	Safari 5.1
	Android 4.0.3	HTC One X	Chrome 18 / Default Android 4 Browser
Symantec Encryption Web Email Protection/Symantec Encryption PDF Email Protection for tablets	iOS 5.1.1	iPad 3	Safari 5.1

Note: Support of Symantec Encryption Web Email Protection/Symantec Encryption PDF Email Protection features may be limited by the functionality of the operating systems.

Symantec Encryption Satellite for Windows Requirements

Note: We now support Microsoft Windows 7 operating systems in PGP Universal Satellite 3.0. As a result, we are ending Symantec Encryption Satellite support for Microsoft Windows 2000 Professional and Microsoft Windows 2000 Server & Advanced Server beginning with PGP Universal Satellite 3.1.

Before you install, you must verify that your system meets these minimum requirements:

- The following Microsoft Windows versions:
  - Windows 8 Enterprise (32- and 64-bit editions)
  - Windows 8 Pro (32- and 64-bit editions)
  - Windows 7 (all 32- and 64-bit editions, including Service Pack 1)
  - Windows Vista (all 32- and 64-bit editions, including Service Pack 2)
  - Windows XP Professional 32-bit (Service Pack 2 or 3)
  - Windows XP Professional 64-bit (Service Pack 2)

Note: The above operating systems are supported only when all of the latest hot fixes and security patches from Microsoft have been applied.

- 512 MB of RAM
- 64 MB hard disk space
- Internet Explorer 6 or greater
- Mozilla Firefox 1.0 and greater

Symantec Encryption Satellite for Mac OS X Requirements

- Apple Mac OS X 10.7.x, 10.8.2, 10.8.3, 10.8.4 (Intel)
- 512 MB of RAM
- 80 MB hard disk space

Supported External Authentication Products

Symantec Encryption Management Server is compatible with the following LDAP directory products:

- Microsoft Active Directory 2010
- Microsoft Active Directory 2008
- Microsoft Active Directory 2003
- Lotus Notes/Domino Directory 7.0
- OpenLDAP 2.3.x

For directory synchronization, Symantec Encryption Management Server supports:

- LDAPv2
- LDAPv3
- LDAPS

For Symantec Encryption Web Email Protection external authentication, Symantec Encryption Management Server supports:

- LDAPv2
- LDAPv3
- RSA Radius Server with RSA Authentication Manager 7.1

Anti-Virus Software Compatibility

For information about antivirus compatibility, see the *Symantec Encryption Desktop for Windows Release Notes* or the *Symantec Encryption Desktop for Mac OS X Release Notes*.

Upgrade/Migration Requirements

You can upgrade your Symantec Encryption Management Server in the following ways:

- **Migration**, where you back up data to an external location, install the new software version from a CD/DVD, and restore your data. For more information about installing from a CD/DVD, see the *Symantec Encryption Management Server Installation Guide*.
- **PUP Update**, where you download and install a PGP Update Package (PUP) file from your Symantec Encryption Management Server's administrative interface. This method automatically preserves your data and system settings. For more information on performing a PUP update, see the *Symantec Encryption Management Server Administrator's Guide*. Not all upgrades are available as PUP update files.
- **Migration and PUP Update**, where you must use both methods. Some upgrades require a migration where you must back up your system, install the new version of the software, and restore your backup. For example, you must migrate before you use a PUP update when you upgrade from version 2.x to 3.2 or later. You must migrate to 3.0.2 SP2 or 3.12 SP2 first. Then install the PUP file; for example, install the 3.3.1 PUP file for Symantec Encryption Management Server 3.3.1.

After the software is installed and the Setup Assistant has started, depending on how you want to restore your data, there are several paths you can take through the setup.

Warning: If you have a hardware token Ignition Key or a Hardware Security Module (HSM), you must contact Technical Support before you migrate to Symantec Encryption Management Server 3.3 or later. Migrating requires that you create a new setting on the upgraded version of Symantec Encryption Management Server before you restore the backup file from your previous system. This setting can only be added through SSH access with the help of Technical Support. If you migrate to version 3.3 or later without adding this preference, you will be locked out of the user interface after the upgrade. As a result, you cannot use your hardware token Ignition Key to unlock your Symantec Encryption Management Server. This can also occur if you upgrade from 3.0.0 to 3.1.0 using a PUP update. If you are using a hardware ignition key, you must edit the settings in your 3.0.0 installation before the update. You do not need to change any settings if you are running version 3.0.1.

To migrate your data from version 2.12 SP4 to Symantec Encryption Management Server version 3.3.1, you need disk space that is 10 times the size of the backup file. (The backup file will be significantly smaller than the original database.) For example, if your version 2.12 SP4 backup file is 1 GB, you should have 10 GB of disk space to allow for the migration and re-expansion of your data into the 3.3.1 database.

The following applies to Symantec Encryption Management Servers that are running as stand-alone systems or clusters:

- Before you upgrade to Symantec Encryption Management Server 3.3.1, you must back up your data and your organization key to an external location.
- You can upgrade to Symantec Encryption Management Server 3.3.1 from these versions:
  - PGP Universal Server 2.12 SP4

    To upgrade from 2.12 SP4, you must back up your data, do a fresh install of 3.0.2 SP2 or 3.1.2 SP2, and restore your backed up data. Then you can do a PUP update to update to version 3.3.1.

    If you are running a version older than 2.12 SP4, you must upgrade to version 2.12 SP4.
  - Version 3.x

    To upgrade from version 3.x, you can do a PUP update to update to version 3.3.1.

Upgrading to Symantec Encryption Management Server 3.3.1

There are two ways to upgrade to Symantec Encryption Management Server 3.3.1.

Note: Upgrading to 3.3.1 requires installing 1 PUP file: PGPUniversal3.3.1.pup.

To upgrade from version 2.12 SP4 to version 3.2.1:

1. Log in to your Symantec Encryption Management Server administrative interface.
2. Back up your data.
3. Upgrade to one of the following versions by performing a fresh install:
   - 3.0.2 SP2
   - 3.1.2 SP2
4. Restore your data.
5. Select **System > Updates**.
6. Upload and install the PGPUniversal3.3.1.pup file for Symantec Encryption Management Server 3.3.1. The Software Updates page displays this new version number.

After the upgrade, the system reboots, updating the kernel.

To upgrade from version 3.x to Symantec Encryption Management Server 3.3.1:

1. Log in to your Symantec Encryption Management Server administrative interface.
2. Select **System** > **Updates**.
3. Upload and install the PGPUniversal3.3.1.pup file for Symantec Encryption Management Server 3.3.1. The Software Updates page displays this new version number.

After the upgrade, the system reboots, updating the kernel.

Upgrade Best Practices

Symantec Corporation recommends that you test your upgrade in a lab environment before changing your production environment.

To test your upgrade in a lab environment:

1. Do one of the following:
   1. Install Symantec Encryption Management Server on a test system.
   2. Upgrade (or migrate) an existing lab system that is running a previous version of Symantec Encryption Management Server.
2. Test the lab system to ensure that your mail policies and other basic server functionality work as expected.
3. Migrate your live environment.

See the *Symantec Encryption Management Server Upgrade Guide* for more information.

Additional Information

See the *Symantec Encryption Satellite Release Notes* installed with Symantec Encryption Satellite for additional information.

Note: Starting with PGP Universal Satellite version 3.2, Microsoft Windows 2000 Professional and Microsoft Windows 2000 Server & Advanced Server are no longer supported.

Installation and Upgrade

- Symantec Encryption Management Server version 3.3.1 does not support host names longer than 64 ASCII characters. In addition, Symantec Encryption Management Server version 3.3.1 does not support gTLD (generic Top Level Domain names).
- If you have a hardware token Ignition Key or a Hardware Security Module (HSM), you must contact Technical Support before you migrate to Symantec Encryption Management Server 3.3. Migrating to version 3.3 requires that you create a new setting on the upgraded (3.3) version of Symantec Encryption Management Server before you restore the backup file from your previous system. This setting can only be added through SSH access with the help of Technical Support. If you migrate to version 3.3 without adding this preference, you will be locked out of the user interface after the upgrade. As a result, you cannot use your hardware token Ignition Key to unlock your Symantec Encryption Management Server. [27062/2472017]
- If you are running PGP Universal Server 3.2 with an older version of PGP Desktop and Certificate Enrollment is enabled, AutoUpdate fails. However, if you want to perform an update of your clients, you must briefly disable certificate enrollment.

  In Symantec Encryption Management Server, do the following:

  1. Select **Consumers > Consumer Policy > Default policy > Consumer Policy Options > General > Edit**.
  2. Deselect the **Notify users of software updates and automatically download** checkbox.

     AutoUpdate is disabled.
  3. On the Directory Synchronization Settings dialog box, select **Deny** Certificate Enrollment and click **Save**.

     Certificate enrollment is disabled.
  4. If necessary, update Symantec Encryption Management Server to have the desired version of Symantec Encryption Desktop
  5. Select the **Notify users of software updates and automatically download** checkbox.

     AutoUpdate is enabled.
  6. In Symantec Encryption Desktop, complete a manual policy update.

     It can take up to 24 hours for the client to download the installer and update itself.
  7. Upgrade Symantec Encryption Desktop to the correct version.
  8. In Symantec Encryption Management Server, in the Directory Synchronization Settings dialog box, select **Allow** Certificate Enrollment and click **Save**.

     Certificate enrollment is enabled. [31480/2476437]
- When you try to join a node to a cluster, this node is locked by the ignition key. As a result, the status of this node in the sponsor node appears as **Pending** even after the join is complete. [30233/2475190]
- During a PUP update, some exceptions appear in the logs. These exceptions have been noted and can be safely ignored. After the PUP update is complete, all services should start up correctly, and no additional exceptions should occur. [31060/2476017]
- Internal user enrollment is not supported in DMZ node if the **Host internal user private keys for Internal Users and Consumer Groups** checkbox is not selected.[30166/2475123]
- When you select a location to save a backup, if you enter non-ASCII characters in the **Backup Name** field, an error message notifies you that your backup is invalid. Because different file systems treat multiple byte characters differently, your backup file name must consist only of alphanumeric characters. [30140/2475097, 18619/2463811]
- In the Cluster logs, when you join a node to a cluster, warning messages appear.

  An example of a warning message is:

  /usr/share/ovid/pgprep/rep-join-collect.py> pg_dump

  These warnings are intended to be informative, and no action is required. [29773/2474729]
- Symantec Patch Distribution Center now provides all binary updates, which replaces PGP update servers. Automatic updates through the PGP update servers are no longer available.[28208/2473164]
- When joining a node to a cluster, if the sponsoring server is busy (for example, while the nightly key maintenance process is running) it can take a long time for the join process to complete. If Symantec Encryption Management Server cannot complete the join at another time, you need to stop crond and possibly shut down the key maintenance process before starting the join. Contact Symantec Corporation Technical Support for help. [27841/2472796]
- Upgrading to PGP Universal Server 3.0 removes LDAP query customization. When you upgrade to PGP Universal Server 3.0 and later, customized LDAP queries must be recreated as necessary. With the enhancements to LDAP support in PGP Universal Server 3.0, LDAP query customization may no longer be needed. [27366/2472321]
- A SSH key created and saved as a file using the PuTTY utility (PuTTYgen) cannot be imported as an Administrator key using the Key File import function. (Select **System > Administrators**, click the administrator name, and click **+** to add an SSHv2 key.) Instead, you must copy the key block from the PuTTY Key Generator and paste it in **Key Block**. [27325/2472280]

- When you reinstall PGP Universal Server 2.7 or later with custom partitions on a computer that already has custom partitions, the installation fails. You must first reinstall without partitions, and reinstall again with custom partitions. [26748/2471702]
- If you back up data from the Primary in a cluster, and restore the data to a new PGP Universal Server 3.0 installation, unless the cluster member has a DNS-resolvable name, you cannot delete old cluster members. [26128/2471081]
- After you add a new member to a cluster, if the sponsoring cluster member fails to immediately contact the new joining cluster member, check the joining cluster member. If this cluster member is waiting for contact from the sponsor, click **Contact** and try again. [25751/2470704]
- After upgrading a server with multiple NICs to PGP Universal 3.0, the NICs may be renamed. [24178/2469129]
- Before you upgrade to PGP Universal Server 3.0 or later, ensure that do you not have internal and external user policies with the same name. If you do, after migration, users will not receive the correct consumer policy. [23885/2468835]
- Restoring a backup of 2.9.1 to a Symantec Encryption Management Server with a different IP address than the one stored in the backup does not change the IP address of the Symantec Encryption Management Server. [19918/2464857]
- When you back up data on one Symantec Encryption Management Server and restore the data to a different Symantec Encryption Management Server, the MAC address information is incorrect. The MAC address on the restored Symantec Encryption Management Server is set to the MAC address of the backed up Symantec Encryption Management Server. You must contact Technical Support to correct the MAC address. [19895/2464834]
- After PUP updates, the screen is formatted incorrectly. You must clear the cache or refresh the browser screen. [18011/2463202]
- Do not use international characters when you specify file names for backup files. [10834/2456016]
- After manually joining a two-node cluster after a restore, the ignition key fails to unlock on the joiner with an existing ignition key previously installed. To work around this issue, remove the ignition key from the joiner before manually performing the join. For information on how to perform the manual join, go to the Symantec Knowledgebase and search for HOWTO75046, "Manually Joining a Cluster." [2733591]

Deployment

- If you enable Symantec Encryption Management Server to control the Notifier settings for managed Symantec Encryption Desktop clients, the server-specified settings take effect as soon as policy is downloaded to the client. However, the Notifier button on the client continues to appear until the user restarts the desktop client. [27100/2472055]
- If you have a large database, exporting a large data set may take a long time. For example, exporting large sets of Symantec Encryption PDF Email Protection Certified Delivery Receipts takes a long time and generates an exception in the Administrative logs. It may be necessary to use the command line to execute a query against the database. For more details, go to the Symantec Knowledgebase and search for TECH149839, "Unable to Export Large Amount of Reporting Data". [27076/2472031]
- When Symantec Encryption Management Server runs in Learn Mode, it annotates inbound messages, even if the inbound mail policy chain disables notation. After you turn off Learn Mode, mail policy is applied and inbound messages are annotated correctly, according to policy. [26870/2471824]
- If a Symantec Encryption Desktop user is moved from the excluded user group to an internal user group, this user may not download policy for the new group and may continue to use the policy that was previously downloaded for the excluded user group. To ensure that this user properly downloads and follows policy, make any update to the policy for the new group. [26263/2471217]
- When you log in in to a new cluster member while the member is in the joining process, some data may not display properly when you navigate through the interface. This happens because data is being replicated and the new cluster member configuration is changing. Log off and wait until the cluster join is complete. [26057/2471010]
- HTTP-based services do not support port numbers higher than 32767. [25784/2470737]
- Symantec Encryption Management Server does not provide out-of-the-box support for LDAP synchronization in environments where multiple LDAP servers contain identical samAccountName values for different users. If your environment contains multiple LDAP domains with some users having identical samAccountName values, contact Technical Support for help on deploying Symantec Encryption Management Server into your environment. [25299/2470251]
- When you install a new client with a new consumer group policy on an existing client computer, and LDAP enrollment is disabled, the user is not moved to the new consumer group that is associated with that policy and does not receive the new policy. You must manually move the user to the correct consumer group. [24898/2469850]
- On the Keyservers page, if you add Symantec Encryption Management Server to its own keyserver list, use the IP address. If you add it using the Symantec Encryption Management Server hostname, key lookups on that keyserver fail. [24698/2469650]
- When you create a mail policy rule to expand the To list for messages to mailing lists, make sure the conditions are in this order:
    1. Recipient domain <is/contains/matches>.
    2. 'Recipient address is mailing list'
    3. 'Mailing list user count is' <greater than/fewer than>

  If the conditions are not in this order, the rule is not applied.

  [23723/2468673]
- In Microsoft Internet Explorer 8, security can be set to a HIGH state, which disables Javascript on most Web pages. When Javascript is disabled, Symantec Encryption Management Server's administrative interface and Symantec Encryption Web Email Protection login will not function. Make security exceptions for Symantec Encryption Management Server in Internet Explorer 8's security settings or use a different browser to access the administrative interface. [23688/2468637]
- When clients with embedded consumer policy enroll it will, if required by policy, attempt to send key reconstruction data to the Symantec Encryption Management Server and fail. [23579/2468527]
- Silent Enrollment is only supported with Server Key Mode. During enrollment with other key modes, the user is prompted to enter a username and passphrase. [22709/2467655]

- When a NIC is set to a custom link mode, rather than auto-negotiate, the network driver no longer advertises other link speeds. Symantec Encryption Management Server requires access to the list of possible link speeds to populate the Network Settings Link Speed menu. If you want to change the Link Speed from a custom setting, and no other custom settings appear, select Auto and restart Symantec Encryption Management Server. After you restart, the Link Speed menu is populated with all available options for the NIC. [19287/2464456]
- MAC ID, MTU, and Link Speed are not applicable to Symantec Encryption Management Server hosted on VMWare because the ESX server controls the network settings. However, when you create a new virtual interface, those settings are automatically populated. If your Symantec Encryption Management Server runs on VMWare and you want to create a new interface or edit an existing interface, you cannot save your changes until you clear the auto-populated MTU, MAC ID, and Link Speed settings. [19810/2464749]
- Organization Keys with Japanese passphrases cannot be imported. [18620/2463812]
- The Silent Enrollment option does not work with existing certificates or keys, such as CAPI and token keys. [16044/2461234]
- You cannot use spaces in the name of the backup FTP server. [15491/2460680]
- Recovery from a Windows PE environment requires the use of a Whole Disk Recovery Token. TPM and hardware token users cannot be authenticated from Windows PE. [15101/2460290]
- To replace an installation of Symantec Encryption Desktop with an embedded policy with an installation of Symantec Encryption Desktop that retrieves policy from Symantec Encryption Management Server, you must first delete the PGP Corporation folder in %ALLUSERSPROFILE%\Application Data. If you do not delete this folder, your new Symantec Encryption Desktop installation will not receive policy from the Symantec Encryption Management Server. [13252/2458440]
- When creating a new group (under **Consumers**), do not use special characters such as <,>,&, ' , or". Use regular alphabetic or numeric characters. [2909579]

PGP Keys

- When searching for keys from a key server that uses SSL authentication (either LDAPS or USP), Symantec Encryption Management Server does not verify the validity of the certificate presented by the keyserver, nor does it verify that the server DNS name matches the DNS name in the presented certificate. If you need assurance that found keys are trusted, enable the **Require verified key** option in the **Send (encrypted/signed)** action in mail policy. [2735979]
- Automatic approval for any Certificate Signing Request (CSR) received by internal users is disabled by default. To change this, and for information on preventing identity spoofing, contact Symantec Technical Support. [31494/2476451]
- After an internal user submits public keys to the Symantec Verified Directory, if you search for the user by **Name**, you cannot find the user. There are no issues when you search by **Email** or **Name or Email**. [30694/2475651]
- After you enroll an internal user to a configured certificate policy, although the enrollment completes without errors, the process results in the following:
    - A managed user without a managed key in Symantec Encryption Management Server.
    - An untrusted user key in the Symantec Encryption Desktop client. [30354/2475311]
- The **Generate AD Group Keys** dialog box in the **Managed Keys** page does not currently support selecting of Active Directory group names with non-ASCII characters. The operation fails if a non-ASCII name is selected. [30000/2474957]
- When an external user performs a LDAP lookup against an internal user who has both the Lotus Notes and the SMTP address, the Lotus Notes address may be returned. This may result in some email clients refusing to encrypt to the returned X.509 certificate. [29293/2474249]
- After internal user A sends an email to an internal user B, if you revoke a non-SKM key for internal user A, the key displays as valid until after your regular cron job. After the cron job is complete, the key displays as revoked. There are no issues when you revoke SKM keys. [29026/2473982]
- On the **Clustering** page, if you deselect the **Host private keys for internal users and Consumer Groups** checkbox in the **Add/Edit Member** dialog box, and then reselect it, saving after each selection, the cluster member repopulates the Managed Key database with the private keys. However, the indices to the keys are erased and not rebuilt.

  Although the server can still perform functions, such as encrypting and decrypting email, it cannot display the existing managed keys. As a result, key lookup requests through the user interface, Verified Key Directory, or LDAP on that cluster node fail. This does not affect the key management features on other cluster members, and you can still display and search for keys on those nodes. On the **Managed Key** page, if a cluster node is unable to display the existing keys, we recommend that you remove the node from the cluster and add it back as soon as possible. [25906/2470859]
- Signature operations may download the private portion of the MAK key to the managed Symantec Encryption Desktop, even if the key is SKM. These operations include signing a document and validating the signature on a document. Downloading the private portion of certain types of keys may be a security problem in some environments. [26106/2471059]
- On the **Managed Keys** page, the name associated with a managed key should be the primary email address associated with the key, not the last listed email address. [25115/2470067]
- Exporting or deleting tens of thousands of user keys at a time can take hours, or can fail. Export fewer keys at a time, or contact Symantec Corporation Technical Support for help. [15998/2461188]
- When making any changes that affect which TLS client certificates are permitted to access the Keyserver service, you must disable, and re-enable the Keyserver service for these changes to take effect. [6533/2451708]

Messaging

- To make the exported delivery receipts file for Certified Delivery display Japanese characters correctly, you must save the file as UTF-8:

  1. Export the CSV file.

2. Open the file as UTF-8 with an editor that supports UTF-8 and click **Save**.

The file converts to UTF-8 format. [24466/2469418]

- When an imported external user key is used to encrypt outgoing messages, the logs report that the key was found with in Internal User Keys, rather than External User Keys. [23757/2468707]
- If a user's Thunderbird email client is set to send email in HTML-only format, and the message is encrypted by Symantec Encryption Management Server or Symantec Encryption Desktop before it arrives at the BES gateway, the recipient cannot view the email message on his or her BlackBerry. You must configure the Thunderbird email client to not send HTML-only messages. [16273/2461463]
- When a large Symantec Encryption PDF Email Protection or Symantec Encryption Web Email Protection message is sent out of the mail stream, the connection to the Symantec Encryption Management Server times out before the mail is sent. [15916/2461106]
- Microsoft Windows Mail in Windows Vista may incorrectly deliver the Symantec Encryption Desktop enrollment email message to the Junk E-mail folder, instead of to the Inbox. If you are using that email client in a managed setting, disable the Junk E-mail feature. [13149/2458337]
- Microsoft Outlook 2007 uses extensive processing time to handle extremely large HTML attachments. The connection with the Symantec Encryption Management Server may time out before the message can be sent. [12545/2457732]
- Characters added in versions of Unicode after 3.0 are not supported in Symantec Encryption Management Server Dictionaries. [10367/2455549]
- Some of the more obscure authentication methods for POP/IMAP/SMTP may not work through Symantec Encryption Management Server. We recommend that you always activate SSL/TLS between your client machines and Symantec Encryption Management Server. If you also deploy Symantec Encryption Satellite internally, Symantec Encryption Satellite automatically probes for SSL/TLS on the server and upgrade mail connections to use SSL/TLS whenever possible. Plain, Login, MSN, NTLM, and CRAM-MD5 authentication are officially supported in this release. [NBN]
- Stalker's CommuniGate Pro mailserver contains a MAPI client adapter to redirect MAPI over IMAP. This adapter is not currently compatible with Symantec Encryption Satellite. [2430/2447597]
- If a message is encrypted by PGP Notes, the "Encrypt" button rule on Symantec Encryption Management Server does not work. This is because the Lotus Domino SMTP gateway strips out all non-standard X headers. [2688138]
- Symantec Encryption Desktop is unable to decrypt mail sent from Symantec Mobile Encryption when Symantec Encryption Desktop is connected to Microsoft Exchange Server 2007 or 2010 using the IMAP protocol. This is due to a limitation in Microsoft Exchange Server 2007 and 2010. [2962760]

Symantec Encryption Web Email Protection

- Due to a security fix implemented by Microsoft (10.0.9200.16635), Web Email Protection users who exit their session by clicking the Close button (X) instead of logging out using the Logout link remain logged in to their session. The default timeout for this is 15 minutes, however you can change this setting by changing the properties settings. Note that this setting also affects the timeout on inactivity however. For more information, go to the Symantec Knowledgebase and search for TECH208847 "Symantec Encryption Management Server 3.3.1 Modifying Web Email Protection Time Outs." [3253004/3263910]
- If you create a Complete Customization template and name it so that it is inserted between two existing Simple Customized templates, the **Download** icon only appears for the Complete Customization template and the templates that appear after it. To download the Simple Customization template that appears before the Complete Customization template, you must mouse over the Simple Customization template for download instructions. [30877/2475834]
- Depending on your Microsoft Windows version, opening files with non-Latin filenames directly from Symantec Encryption Web Email Protection may result in garbled filenames. To avoid this problem, save attachments to your desktop before you open them. [12011/2457196]
- Replies to Symantec Encryption Web Email Protection email messages may not work if a load balancer is directing traffic for the untrusted interfaces of a cluster of Symantec Encryption Management Servers in gateway placement. You can disable rules your hardware may enforce to prohibit traffic to a virtual server from a member of the load balancing pool. Check with your hardware vendor to determine if this is possible. [NBN]
- Symantec Encryption Web Email Protection mailbox quotas of up to 2 GB are supported for this release. [7986/2453164]

Symantec Drive Encryption

- **Using embedded policy with PGP WDE command line:** You cannot encrypt a disk using the PGP WDE command line if you have customized Symantec Encryption Desktop with the Preset Policy Group with Embedded Policy option. To use preset policy, you must install Symantec Encryption Desktop using the user interface. [2871587]
- When customizing the PGP BootGuard screen, enter a maximum of 79 characters (if using UTF-8 characters). Exceeding this number of characters results in a truncated line of text in the PGP BootGuard screen. [2660786]
- Disabling the Enable Whole Disk Recovery Tokens Consumer Policy setting does not work for Symantec Encryption Desktop for Mac OS X. Whole Disk Recovery Tokens are still sent to Symantec Encryption Management Server. [28397/2473353]
- If consumer policy requires disk encryption, but the user pauses the encryption process and then decrypts the disk, Symantec Encryption Desktop for Windows does not immediately prompt the user to re-encrypt the disk. The encryption prompt appears after the user restarts PGP Tray or logs out and then logs back in again. [28393/2473349]
- When you upgrade clients from PGP Universal Server 2.x, if you want these clients to use local self-recovery, you must force client re-enrollment. [27863/2472818]
- Symantec Encryption Management Server's log files do not show when a user logs in to an encrypted computer using Local Self-Recovery. [27829/2472784]

- On the Symantec Drive Encryption Computers page, the status of partially encrypted disks appears as None encrypted. [26825/2471779]
- In the Client log, bad sector log entries do not report the correct number of bad sectors and may erroneously report 0. When no bad sectors are encountered, there are no log entries that refer to bad sectors. [18105/2463297]
- The Symantec Drive Encryption Force Encrypt setting is not set and enforced correctly after an upgrade. If you use this option, review and verify your policy, because you will have more settings you can select. [17793/2462984]
- Symantec Encryption Management Server does not validate images uploaded for use with PGP BootGuard. For more information on creating, uploading, and testing images, see the Knowledge Base. [15457/2460646]

Symantec File Share Encryption

- Certain characters that are allowed when you create Active Directory groups can cause Symantec File Share Encryption to fail on encryption, re-encryption, or searches. Do not use the pound, percent, or left/right parentheses [#, %, (, or)] when you create Active Directory groups. [26336/2471290]
- Symantec File Share Encryption is not updated when you replace your Organization ADK with a new ADK. You must re-encrypt the Symantec File Share Encryption folder to the new ADK. [22866/2467812]
- Files protected by application-based encryption policy (white-listed applications) are locked after the user who is associated with the policy, logs off or shuts down the system. These files require authentication to access them. [17491/2462682]

Getting Assistance

Available Documentation

Symantec Encryption Management Server 3.3.1 documentation is available in the following formats:

- On the Documentation disk and in the Symantec Encryption Management Server administrative interface.
- Online help on each page in the administrative interface. Prior to installation, complete Product Documentation is available through the Symantec Corporation Support Portal.
- As a PDF file.

  To view or print PDF files, you need Adobe Acrobat Reader, which is available on the Documentation disk and from the Adobe website.

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level

- Network topology
- Router, gateway, and IP address information
- Problem description:
    - Error messages and log files
    - Troubleshooting that was performed before contacting Symantec
    - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, Africa	semea@symantec.com
North America, Latin America	supportsolutions@symantec.com

Copyright and Trademarks

Copyright (c) 2013 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, PGP, Pretty Good Privacy, and the PGP logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.